世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G09C 1/00, H04L 9/06	A1	(11) 国際公開番号	WO99/00783
		(43) 国際公開日	1999年1月7日(07.01.99)

(21) 国際出願番号 PCT/JP98/02915

(22) 国際出願日 1998年6月30日(30.06.98)

(30) 優先権データ
特願平9/173672 1997年6月30日(30.06.97) JP

(71) 出願人（米国を除くすべての指定国について）
日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION)[JP/JP]
〒163-8019 東京都新宿区西新宿三丁目19番2号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
神田雅透(KANDA, Masayuki)[JP/JP]
高嶋洋一(TAKASHIMA, Youichi)[JP/JP]
〒163-1419 東京都新宿区西新宿3丁目20-2
日本電信電話株式会社内 Tokyo, (JP)
青木克彦(AOKI, Katsuhiko)[JP/JP]
〒107-0062 東京都港区南青山5-11-5 Tokyo, (JP)
松本 勉(MATSUMOTO, Tsutomu)[JP/JP]
〒227-0048 神奈川県横浜市青葉区柿の木台13-45
Kanagawa, (JP)

(74) 代理人
弁理士 草野 卓, 外(KUSANO, Takashi et al.)
〒160-0022 東京都新宿区新宿四丁目2番21号 相模ビル
Tokyo, (JP)

(81) 指定国 CA, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

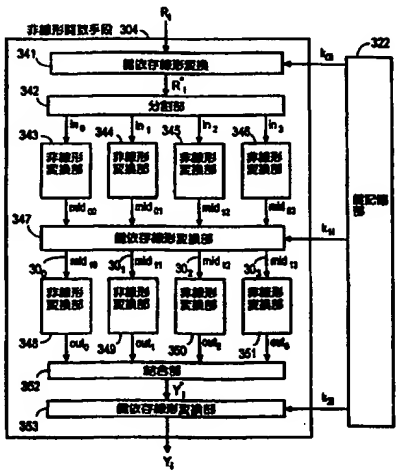
添付公開書類
国際調査報告書

(54)Title: CIPHERING APPARATUS

(54)発明の名称 暗号装置

(57) Abstract

A ciphering apparatus of common key type, wherein a plurality of rounding units are connected in cascade, the i-th rounding unit is fed with input data L_i, R_i, the input data R_i are subjected to nonlinear transformation by a nonlinear function unit depending upon the key data, the exclusive-OR output of the output of the nonlinear function unit and the input data L_i is outputted as data R_{i+1} to the (i+1)-th rounding unit, and the input data R_i are outputted as data L_{i+1} to the (i+1)-th rounding unit. The nonlinear function unit includes: a key-dependent linear transforming unit for subjecting the input R_i to key-dependent linear transformation; a dividing unit for dividing the output into four data in_0, in_1, in_2 and in_3; first nonlinear transforming units for subjecting the divided data to nonlinear transformation to output data mid_{00}, mid_{01}, mid_{02} and mid_{03}; a key-dependent linear transforming unit for correlating these transformed outputs to each other and subjecting them to linear transformation based upon the key data to output data mid_{10}, mid_{11}, mid_{12} and mid_{13}; second nonlinear trasnforming units for subjecting the transformed outputs to nonlinear transformation to output data out_0, out_1, out_2 and out_3; and a coupling unit for coupling the transformed outputs to output data Y.



(57)要約

共通鍵型の暗号装置において、複数段のラウンド処理部が従属接続して設けられ、各ｉ段のラウンド処理部は入力データL_i，R_iが与えられ、入力データR_iを非線形関数部により鍵データに応じて非線形変換し、その出力と、入力データL_iとの排他的論理和出力を次段に与えるデータR_{i+1}として出力し、入力データR_iを次段に与えるデータL_{i+1}として出力し、各段の非線形関数部は、入力R_iを鍵依存線形変換する鍵依存線形変換部と、その出力を４つのデータin_0，in_1，in_2，in_3に分割する分割部と、これら分割データをそれぞれ非線形変換してデータmid_{00}，mid_{01}，mid_{02}，mid_{03}を出力する第１の非線形変換部と、これら変換出力を互いに関連づけると共に、鍵データに基づいてそれぞれ線形変換してデータmid_{10}，mid_{11}，mid_{12}，mid_{13}を出力する鍵依存線形変換部と、それらの変換出力をそれぞれ非線形変換し、データout_0，out_1，out_2，out_3を出力する第２の非線形変換部と、それらの変換出力を結合しデータＹを出力する結合部とを含む。

明細書

暗号装置

技術分野

この発明は、データの通信または保持において、データを秘匿するための暗号化装置、特に、秘密鍵の制御のもとでデータをブロック単位で暗号化または復号を行う共通鍵暗号方式による暗号化装置に関するものである。

従来の技術

データを秘匿するための暗号化装置に含まれる代表的な共通鍵暗号方式には、米国連邦標準暗号であるＤＥＳ（Data Encryption Standard）暗号がある。

図１は、ＤＥＳ暗号の機能構成を示す。ＤＥＳ暗号では、５６ビットの秘密鍵を用い、６４ビットのデータブロック単位に暗号化または復号を行う。図１において、暗号化処理は、平文Ｐの６４ビットを初期変転部１１において初期転値で変換した後、３２ビットごとのブロックデータL_0，R_0に分割される。ブロックデータR_0は図２に第ｉ段ラウンド処理部14_i（i=0, 1, …, 15）のものとして示す関数演算部（ラウンド関数と呼ばれている）１２へ入力され、４８ビットの拡大鍵k_0の制御のもとに$f(R_0, k_0)$に変換される。この変換データ$f(R_0, k_0)$とブロックデータL_0との排他的論理和をＸＯＲ回路１３でとり、その出力とブロックデータR_0とを入れ替えて、次のブロックデータL_1，R_1とする。即ち、

$$R_1 = L_0 \oplus f(R_0, k_0)$$
$$L_1 = R_0 \qquad (1)$$

である。

このように２つのブロックデータL_0，R_0を入力として演算部１２と排他的論理和回路１３とデータの入れ替え（スワップ）とによりL_1，R_1を出力する第０段ラウンド処理部14_0が構成され、同じようなラウンド処理部14_1～14_{15}が縦続的に設けられる。第ｉ段ラウンド処理部14_iによる処理を第ｉ段のラウンド処理と呼ぶことにする。ただし、i=0, …, 15 である。つまり各ラウンド処理部14_i（$0 \leqq i < 15$）では、

$$R_{i+1} = L_i \oplus f(R_i, k_i)$$

$$L_{i+1}=R_i \qquad (2)$$

の処理が行われ、最後にR_{16}，L_{16}を統合して６４ビットにした後、最終転値部１５において最終転値で変換して暗号文６４ビットを出力する。復号処理においては、関数ｆに入力する拡大鍵k_0，k_1，…，k_{14}，k_{15}の順序だけを逆転させて、k_{15}，k_{14}，…，k_1，k_0の順に入力するようにする点を除けば、暗号化処理と同じ手順で実行できる。その場合、最終段ラウンド処理部１４$_{15}$のスワップ出力L_{16}，R_{16}を、図に示すように更にスワップするように構成することにより、復号処理において暗号文を初期転置１１に入力して図１の処理を実行することにより、最終転置１５の出力に平文がそのまま得られる。勿論、最終段ラウンド処理部１４$_{15}$の出力をスワップしないで最終転置１５にデータを与える構成としても全く同じである。なお、拡大鍵k_0，k_1，…，k_{14}，k_{15}は、暗号化処理とは別の拡大鍵生成ルーチン１６で５６ビットの秘密鍵が４８ビットの拡大鍵１６個の計768 ビットに拡大されることによって生成される。

関数演算内部１２の処理は、図２に示すように行われる。まず、３２ビットのブロックデータR_iは拡大転値部１７で４８ビットデータ$E(R_i)$に変換される。これに拡大鍵k_iとで排他的論理和をＸＯＲ回路１８で取り、４８ビットデータ$E(R_i)\oplus k_i$に変換した後、８個の６ビットごとのサブブロックデータに分割する。この８個のサブブロックデータはそれぞれ異なるS-box S_1～S_8に入力され、各々が４ビットの出力を得る。なお、このS-box S_j(j=1,…,8) は６ビットの入力データから４ビットの出力データに変換する非線形変換テーブルであり、ＤＥＳ暗号の本質的な安全性を担っている部分である。S-box S_1～S_8の８つの出力データは、再び連結されて３２ビットデータになった後、転置変換部１９を経て、図８に示されるように、L_iと排他的論理和される関数ｆの出力$f(R_i, k_i)$となる。

次に、暗号解読法について述べる。ＤＥＳ暗号を始めとする従来の共通鍵暗号方式についてはさまざまな方面から暗号解読が試みられており、そのなかでも、極めて効果的な解読法であるのがＥ．Biham 及びＡ．Shamirによって提案された差分解読法（“Differential Cryptanalysis of DES-like Cryptosystems.”Proceedings of CRYPTO'90）と松井によって提案された線形解読法（“ＤＥＳ暗号

の線形解読法（Ｉ），”１９９３年暗号と情報セキュリティシンポジウムSCIS93-3C）である。

差分解読法は、２つのデータＸ，Ｘ* の差分を

$$\Delta X = X \oplus X^* \qquad (3)$$

としたとき、解読者が入手している平文・暗号文の２組を以下の式に適用して、最終ラウンドにおける拡大鍵k_{15}を求めることを目的としている。図１の暗号化処理において、既知の第１平文を入力したときの各ラウンド処理部14_iでの入力ブロックデータをL_i，R_iとし、既知の第２平文を入力したときの各ラウンド処理部14_iでの入力ブロックデータをL^*_i，R^*_iとする。これら第１及び第２平文が入力されたときの出力暗号文がそれぞれ既知であるとする。上記式(3) の定義により

$$\Delta L_i = L_i \oplus L^*_i$$

$$\Delta R_i = R_i \oplus R^*_i \qquad (4)$$

である。図１において、$L_{15}=R_{14}$，$L^*_{15}=R^*_{14}$，$L_{16}=R_{15}$，$L^*_{16}=R^*_{15}$なので、

$$R_{16} = L_{15} \oplus f(R_{15}, k_{15})$$

$$R^*_{16} = L^*_{15} \oplus f(R^*_{15}, k_{15}) \qquad (5)$$

が成立し、これら２つの式の両辺の排他的論理和を取ると

$$\Delta R_{16} = \Delta L_{15} \oplus f(L_{16}, k_{15}) \oplus f(L_{16} \oplus \Delta L_{16}, k_{15}) \qquad (6)$$

が得られ、その両辺と$\Delta R_{14}=\Delta L_{15}$との排他的論理和を取ることにより次の式が得られる：

$$f(L_{16}, k_{15}) \oplus f((L_{16} \oplus \Delta L_{16}), k_{15}) = \Delta R_{16} \oplus \Delta R_{14} \qquad (7)$$

このとき、L_{16}，ΔL_{16}，ΔR_{16}は暗号文から得られるデータであるので既知の情報である。このため、解読者がΔR_{14}を正しく求めることができるならば、上式はk_{15}のみが未知定数となり、既知の平文・暗号文の組を用いてk_{15}に関する全数探索を行うことで、解読者は必ず正しいk_{15}を見つけだすことができる。一方、ΔR_{14}についてみてみると、この値は中間差分値であるため、一般には求めることが困難である。そこで、０ラウンド目から最終ラウンドの一つ前までのラウンド目までにおいて、各ラウンドが確率p_iで

$$\Delta R_{i+1} = \Delta L_i \oplus \Delta\{f(\Delta R_i)\}$$

$$\Delta L_{i+1} = \Delta R_{i+1} \qquad (8)$$

のように近似されるとおく。ここでのポイントは、あるΔR_iが入力されたとき、拡大鍵k_iの値に関わらず、確率p_iでΔ{f(ΔR_i)}を予測できるということにある。このように近似できるのは、Δ{f(ΔR_i)}に影響を与えるのが非線形な変換であるS-boxの部分だけであり、しかもS-boxにおいて、入力差分によっては差分出力の分布に極めて大きな偏りが生じるためである。例えば、S-box S_1では、入力差分"110100"のとき、1/4の確率で出力差分"0010"に変換されるためである。そこで、各々のS-boxが確率$p_{s,i}$で入力差分と出力差分との関係が予測できるとおき、これらを組み合わせることで各ラウンドの近似を求める。更に、各ラウンドでの近似を連結していくことで、ΔR_{14}は確率$P=\Pi p_i$でΔL_0, ΔR_0(ΔL_0, ΔR_0は平文から得られるデータであるので既知の情報である）から求められることになる。なお、この確率Pが大きいほど、暗号解読が容易である。このようにして、拡大鍵k_{15}が求められると、今度は1段少ない15段DES暗号とみなして、同様の手法で、拡大鍵k_{14}を求めていくということを繰り返して、最終的に拡大鍵k_0まで求めていく。

Bihamらによると、この解読法では、2^{47}組の選択された既知平文・暗号文の組があればDES暗号を解読できるとしている。

また、線形解読法は、以下の線形近似式を構成し、解読者が入手している平文・暗号文の組による最尤法を用いて拡大鍵を求めることを目的としている。

$$(L_0, R_0)\cdot\Gamma(L_0, R_0)\oplus(L_{16}, R_{16})\cdot\Gamma(L_{16}, R_{16})$$
$$=(k_0, k_1, \cdots, k_{15})\cdot\Gamma(k_0, k_1, \cdots, k_{15}) \qquad (9)$$

ただし、Γ(X)はXの特定のビット位置を選択するベクトルを表し、マスク値という。

線形近似式の役割は、暗号アルゴリズム内部を線形表現で近似的に置き換え、平文・暗号文の組に関する部分と拡大鍵に関する部分とに分離することにある。つまり、平文・暗号文の組に関して、平文の特定のビット位置の値と暗号文の特定のビット位置の値との全ての排他的論理和が一定値となり、その値は拡大鍵の特定のビット位置の値の排他的論理和に等しくなることを表している。従って、解読者は

$(L_0, R_0) \cdot \Gamma(L_0, R_0) \oplus (L_{16}, R_{16}) \cdot \Gamma(L_{16}, R_{16})$

の情報から

$(k_0, k_1, \cdots, k_{15}) \cdot \Gamma(k_0, k_1, \cdots, k_{15})$ （１ビット）

の情報が得られるということになる。このとき、(L_0, R_0), (L_{16}, R_{16})はそれぞれ平文・暗号文のデータであるので既知の情報である。このため、解読者が$\Gamma(L_0, R_0)$, $\Gamma(L_{16}, R_{16})$, $\Gamma(k_0, k_1, \cdots, k_{15})$ を正しく求めることができるならば、$(k_0, k_1, \cdots, k_{15}) \cdot \Gamma(k_0, k_1, \cdots, k_{15})$（１ビット）を求めることができる。

ＤＥＳ暗号では、非線形な変換が行われるのはS-box においてだけであり、従ってS-box についてのみ線形表現ができれば、容易に線形近似式が構成できる。そこで、各々のS-box S_i が確率p_{s_i}で線形表現できるとおく。ここでのポイントは、S-box に対する入力マスク値が与えられたとき、確率p_{s_i}でその出力マスク値を予測できるということにある。これは、非線形変換テーブルであるS-boxにおいて、入力マスク値によっては差分マスク値の分布に極めて大きな偏りが生じるためにおこる。例えば、S-box S_5 では、入力マスク値"010000"のとき、3/16の確率で出力マスク値"1111"が予測されるためである。これらS-box におけるマスク値を組み合わせることによって、各ラウンドが確率p_i で入力マスク値と出力マスク値のあいだに線形近似することができ、各ラウンドでの線形近似を連結していくことで、$\Gamma(L_0, R_0)$, $\Gamma(L_{16}, R_{16})$, $\Gamma(k_0, k_1, \cdots, k_{15})$ は確率

$$P = 2^{n-1} \Pi |p_i - 1/2| \qquad (10)$$

で求められることになる。なお、この確率Ｐが大きいほど、暗号解読が容易である。

松井によると、この解読法で、2^{43}組の既知平文・暗号文の組を用いて、ＤＥＳ暗号の解読に成功している。

さて、上記の解読法に対抗するためには、確率Ｐが十分に小さくなればよい。このため、確率Ｐを小さくするための提案がさまざま行われており、なかでも従来の暗号方式において、もっとも簡単に安全性を高めるための方法がラウンド数を増やすことであった。例えば、ＤＥＳ暗号を３つつなげたTriple-DES暗号は、実質的にＤＥＳのラウンド数を１６段から４８段に増やした暗号方式であり、確

率Ｐは、ＤＥＳ暗号よりもはるかに小さい。

しかし、上記の解読法に対抗するための対策として、ラウンド数を増加させることは、暗号装置の規模が大きくなり、データの処理量も増加することになる。例えば、ラウンド数を３倍に増やせば、暗号化処理量も３倍になる。つまり、現在のＤＥＳ暗号の暗号化速度はPentium ＰＣクラスで約10Mbpsであるため、Triple－ＤＥＳ暗号ともなると約3.5Mbps まで暗号化速度が低下する。一方で、ネットワークやコンピュータなどは年々高速化しており、暗号化装置もそれらの高速化に対応したものが望まれている。このため、従来の暗号装置では、それらの高速化の要求に対して、安全性と高速性を同時に満たすことはきわめて困難な状況になっている。

この発明の目的は、上記の点を鑑みなされたもので、ラウンド段数を増加させることなく安全性条件を満たすような暗号装置を提供することにある。

発明の開示

この発明では、特に非線形関数部において、非線形関数部の入力データに鍵記憶部に保持された鍵データに基づいて線形変換を行う鍵依存線形変換部と、この鍵依存線形変換部の出力データを複数個のビット列に分割する分割部と、これら分割された各ビット列に非線形変換をそれぞれ行う第１の非線形変換部と、その第１の非線形変換部の各々の出力ビット列間で線形変換を行う第１の線形変換部と、その第１の線形変換部の出力ビット列の一部またはすべてに非線形変換を行う第２の非線形変換部と、その第２の非線形変換部の出力ビット列をその非線形関数部の出力データに結合する結合部とを備えることを特徴とする。

更に安全性を向上させるには、上記結合部の出力データを上記非線形関数部の出力データに線形変換を行う第２の線形変換部を備えることを特徴とする。

また、上記第１の線形変換部または上記第２の線形変換部、もしくはその両方の部が、データの線形変換を行うときに、上記鍵記憶部に保持された鍵データに基づいて線形変換を行う鍵依存線形変換部であることを特徴とする。

この発明によれば、S-box における確率が$p_i \leqq p_b < 1$であるとき（p_bはS-box の最大差分又は線形確率）、各ラウンドを近似するときの確率は$p_i \leqq p_b^2$（ただし、差分解読法の場合は関数ｆへの入力差分が０でないとき、線形解読

法の場合は関数ｆでの出力マスク値が０でないとき）となることが保証される。また、関数ｆが全単射（入力が異なれば出力が必ず異なる）であるとき、暗号方式のラウンド数を３ｍとすると、暗号方式としての確率は$P \leqq p_i^{2m} \leqq p_b^{4m}$となる。一般に、暗号方式では$P < 2^{-64}$であれば差分解読法や線形解読法に対して安全とされるため、$m > -16/\{\log_2(p_b)\}$を満たせばよく、$p_b \leqq 2^{-4}$であればＤＥＳ暗号の１６ラウンドよりも少ないラウンド数で安全性を確保できる。なお安全性の確率はｍラウンドの倍数ごとに変化する。

この発明によれば、差分解読法や線形解読法に対する安全性を比較的少ないラウンド数で確保できるため、安全性と低処理量を両立させた暗号装置を提供することが可能になる。

図面の簡単な説明

図１は従来のＤＥＳ暗号装置の機能構成を示す図。

図２は図１中のｆ関数演算部１２の具体的機能構成を示す図。

図３はこの発明の実施例１の機能構成を示す図。

図４は実施例１における非線形関数部304 の詳細な機能構成例を示す図。

図５は図４中の鍵依存線形変換部347 の具体例を示す図。

図６はこの発明の実施例２の機能構成を示す図。

図７Ａは実施例２における非線形関数部304 の詳細な機能構成を示す図。

図７Ｂはこの非線形関数部304 における線形変換部354 の具体例を示す図。

図８はこの発明の実施例３の機能構成を示す図。

図９は実施例３における非線形関数部304 の詳細な機能構成を示す図。

発明を実施する最良の形態

実施例１

以下、この発明の一実施例を図面を用いて説明する。

図３は、この発明の一実施例を示す暗号装置における、暗号化処理手順の機能構成を示したものである。この発明による暗号装置においても、入力データを２つのブロックデータL_0，R_0に分割し、それらを順次ラウンド処理するｎ段に従属

接続されたラウンド処理部３８$_0$～３８$_{n-1}$が設けられ、各ラウンド処理部３８$_i$（i=0, 1, …, n-1）は図１のラウンド関数部１２に対応する非線形関数部304 と、図１のＸＯＲ回路１３に対応する線形演算部305 と、交換部306 とから構成されている。

平文に相当する入力データＰを入力部301 から暗号装置内に入力する。予め、鍵入力部320 から入力されたデータに基づいて鍵データ生成部321 により鍵データ

{fk; k_{00}, k_{10}, k_{20}; k_{01}, k_{11}, k_{21}; …; $k_{0(n-1)}, k_{1(n-1)}, k_{2(n-1)}$; ek}

が生成され、鍵記憶部322 に保持される。入力平文データＰは鍵記憶部322 に保持されている鍵データｆｋによる鍵依存初期線形変換部302 で変換された後、初期分割部303 で２つのブロックデータL_0, R_0に分割される。例えば６４ビットのデータが３２ビットづつのブロックデータL_0, R_0に分割される。ブロックデータR_0 は、鍵記憶部322 に保持されている鍵データk_{00}, k_{10}, k_{20}と共に第０段ラウンド処理部３８$_0$ の非線形関数部304 に入力され、変換処理によりデータＹ$_0$ に変換される。データＹ$_0$ とブロックデータＬ$_0$ は線形演算部305 で演算されてデータL_0^* に変換される。データL_0^* とブロックデータR_0 は交換部306 でデータ位置の交換（スワップ）が行われ、$L_1 = R_0$, $R_1 = L_0^*$ とされ、L_1, R_1が次の第１段ラウンド処理部３８$_1$ に入力される。

以下、第ｉ段ラウンド処理部３８$_i$(i=1, …, n-1）において、２つの入力ブロックデータL_i, R_iについて上記と同様の処理を繰り返し行う。即ち、第ｉ段ラウンド処理部３８$_i$ においては、２つのブロックデータL_i, R_iのうちの、データR_i は、鍵記憶部322 に保持されている鍵データk_{0i}, k_{1i}, k_{2i}と共に非線形関数部304 に入力され、非線形関数部304 で変換処理を受け、データＹ$_i$ に変換される。データＹ$_i$ とブロックデータＬ$_i$ は線形演算部305 で演算されてデータL_i^* に変換される。データL_i^* とデータR_i は交換部306 でデータ位置の交換が行われ、$L_{i+1} = R_i$, $R_{i+1} = L_i^*$ のように交換される。線形演算部305 は例えば排他的論理和演算を行うものである。

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、ラウンド処理部38$_0$～38$_{n-1}$による繰り返し処理の結果、データL_n, R_nが得られる。

このデータL_n，R_nを最終結合部307 で１つのブロックデータに結合し、つまり例えば３２ビットの各L_n，R_nをビット結合して６４ビットのデータとし、その後、鍵記憶部322 に保持されている鍵データｅｋを使って鍵依存最終線形変換部308で変換し、出力部309 から暗号文として出力データＣを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。例えば図３において入力データの代りに暗号文データを入力し、鍵データを図３とは逆に、ek，$k_{0(n-1)}$，$k_{1(n-1)}$，$k_{2(n-1)}$，…，k_{01}，k_{11}，k_{21}，k_{00}，k_{10}，k_{20}，fk を順次与えればよい。

図４は、各ラウンド処理部３８$_i$ に使用されている非線形関数部304 の機能構成を示す。第ｉ段ラウンド処理部３８$_i$ の入力ブロックデータＲ$_i$ は、鍵記憶部322 に保持されている鍵データk_{0i}，k_{1i}，k_{2i} と共に非線形関数部304 への入力データとなる。ブロックデータＲ$_i$ は、鍵データk_{0i}を使用した鍵依存線形変換部341 によりデータR_i^* に線形変換される。データR_i^* は分割部342 において例えば８ビットづつの４つのデータin_0，in_1，in_2，in_3にビット分割される。４つのデータin_0，in_1，in_2，in_3は、それぞれ非線形変換部343，344，345，346において、データ$mido_0$，$mido_1$，$mido_2$，$mido_3$に非線形変換された後、鍵依存線形変換部347 に入力される。

鍵依存線形変換部347 は、図５に示すようにこの例ではそれぞれが少なくとも１つの排他的論理和を含む４つの処理系列３０$_0$～３０$_3$から構成され、これら処理系列はそれらの排他的論理和により互いに論理結合されている。各処理系列において他の処理系列のデータと線形演算（排他的論理和）を行うことにより、それぞれの処理系列において均質化されたデータを生成し、図５の例では更に鍵データk_{1i}により線形処理される。即ち、データ$mido_0$，$mido_1$，$mido_2$，$mido_3$はそれぞれ処理系列３０$_0$ ～３０$_3$ に入力され、処理系列３０$_1$ において入力データ$mido_0$と$mido_1$との排他的論理和がＸＯＲ３１$_1$ によりとられ、また処理系列３０$_2$ において入力データ$mido_2$と$mido_3$の排他的論理和がＸＯＲ３１$_2$ によりとられ、更にＸＯＲ３１$_1$ の出力とＸＯＲ３１$_2$ の出力の排他的論理和がＸＯＲ３２$_2$ によりとられる。ＸＯＲ３１$_1$ の出力とＸＯＲ３２$_2$ の出力との排他的論理和がＸＯＲ３３$_1$ によりとられ、ＸＯＲ３３$_1$ の出力と入力データ$mido_0$ の排他的論理

和がＸＯＲ３４$_0$によりとられ、ＸＯＲ３２$_2$の出力と入力データmid$_{03}$との排他的論理和がＸＯＲ３４$_3$によりとられる。更に、ＸＯＲ３４$_0$，３３$_1$，３２$_2$，３４$_3$のそれぞれの出力と鍵データk$_{110}$，k$_{111}$，k$_{112}$，k$_{113}$との排他的論理和がＸＯＲ３５$_0$～３５$_3$によりとられて、それぞれmid$_{10}$，mid$_{11}$，mid$_{12}$，mid$_{13}$が出力される。つまり処理系列３０$_0$～３０$_3$の入力データmid$_{00}$，mid$_{01}$，mid$_{02}$，mid$_{03}$は相互に関連づけられた後、それぞれ鍵データk$_{110}$，k$_{111}$，k$_{112}$，k$_{113}$に依存した線形変換が行われる。論理式で示すと次式

$$mid_{10} = mid_{00} \oplus mid_{02} \oplus mid_{03} \oplus k_{110}$$

$$mid_{11} = mid_{02} \oplus mid_{03} \oplus k_{111}$$

$$mid_{12} = mid_{00} \oplus mid_{01} \oplus mid_{02} \oplus mid_{03} \oplus k_{112}$$

$$mid_{13} = mid_{00} \oplus mid_{01} \oplus mid_{02} \oplus k_{113} \qquad (11)$$

の論理演算がなされる。これらの式から明らかなように、鍵依存線形変換部３４の各処理系列の出力には少なくとも２つ以上の他の系列の入力データがこの例では排他的論理和の形で含まれており、従って、各系列の出力データには４つの入力データのうち、２つ以上の成分が含まれるように均質化されている。

これら出力データmid$_{10}$，mid$_{11}$，mid$_{12}$，mid$_{13}$は、それぞれの処理系列３０$_0$～３０$_3$に設けられた図４に示す非線形変換部348，349，350，351において、データout$_0$，out$_1$，out$_2$，out$_3$に非線形変換された後、それぞれの処理系列の出力データとして結合部352に与えられ、一つのブロックデータY_i*に結合される。つまり、例えば４つの８ビットデータが１つの３２ビットデータにビット結合される。このデータY_i*は、鍵依存線形変換部353において鍵データk$_{2i}$によりデータY_iに線形変換され、非線形関数部304からの出力データY_iが生成される。非線形変換部343～346，348～351のそれぞれは、例えばＤＥＳ暗号における１つのS-boxと同様のもので、それぞれ入力データに応じた異った出力データを出力する例えばＲＯＭで構成される。

非線形変換部343～346は４つ並列に配置されており、それらの変換処理は相互に関連していないため、これらを並列実行することが可能であり、従って、これらの数が増加することによる処理時間の増大を並列処理により対処できる。非線形変換部348～351についても同様のことがいえる。

各段のラウンド処理部３８$_i$ を構成する線形演算部305（図３）、線形変換部341，347，353（図４）などの処理に要する時間はS-box と同様な非線形変換部343～346，348～351等の処理に要する時間に比べてかなり短いので、暗号化処理に要する時間は使用されるS-box 或いは非線形変換部の数にほぼ比例する。ところが、非線形変換部348～351については、鍵依存線形変換部347 が前述のように複数の入力データを各出力に均質化して出力するため、鍵依存線形変換部347 が、例えば図５のように特定の線形変換であることが予めわかっている場合には、非線形変換部348～351の何れか１つ或いは複数を省略し、対応するデータをそのまま結合部352 に与えても、差分解読法及び線形解読法に対する安全性が低下しないようにすることができ、非線形変換を省略した分だけ暗号化処理量を削減できる。例えば、鍵依存線形変換部347 が図５で表されているとき、非線形変換部349，350を省略し、データmid_{11}，mid_{12}をそのまま結合部352 に入力しても差分解読法及び線形解読法に対する安全性は低下しない一方で、暗号化速度が約３３％向上する。つまり鍵依存線形変換部347 が予め決っている場合は差分解読法、線形解読法に対しては非線形変換部348～351の１つ或いは複数はその存在が安全性に関係ない場合があり、その非線形変換は省略できる。

なお、 図３において、鍵データ生成部321 による鍵データ{fk，k_{00}，k_{10}，k_{20}，k_{01}，k_{11}，k_{21}，…，$k_{0(n-1)}$，$k_{1(n-1)}$，$k_{2(n-1)}$，ek}の生成は図１のＤＥＳ暗号の拡大鍵生成アルゴリズム１６と同様に行うことができる。

上記のように構成された暗号装置の場合、例えば、非線形変換部343～346，348～351の各１つづつが差分解読法及び線形解読法に対して確率$p_b=2^{-6}$で近似表現できるように設計されているならば、各段のラウンド処理部３８$_i$ は非線形変換を必ず２回行うため、即ち、変換部343～346の処理と変換部348～351の処理を縦続して行うため、確率$p_i \leqq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数ｎをｎ＝３ｍとして、確率$P \leqq 2^{-24m}$ で近似表現できることになる。ここで、例えばｍ＝４（ラウンド数１２段）とすると、$P \leqq 2^{-96}$となり、ＤＥＳのラウンド数１６より少ないラウンド数で安全条件$P<2^{-64}$を満たし、差分解読法及び線形解読法に対して十分安全な暗号装置となる。即ち、この発明は、従来のラウンド関数演算部１２（図１）内において非線形変換を縦続して２回行

うように構成することにより、暗号解読に対し安全性を倍に高めることができる。

鍵依存初期線形変換部302 、鍵依存最終線形変換部308 、鍵依存線形変換部347, 353は鍵に依存する線形変換部であるため、差分解読法及び線形解読法以外の解読法に対しても十分な安全性を兼ね備え、もっとも安全性を重視した暗号装置である。

なお、この発明はこの例に特定されるだけでなく、例えば高速性を望むのであれば、後述の実施例のようにこれら鍵依存初期線形変換部302 、鍵依存最終線形変換部308 、鍵依存線形変換部353 については、そのいずれか、もしくはすべてを省略することが可能である。この場合、差分解読法及び線形解読法に対する安全性は低下しない一方で、削除した分だけ暗号化処理速度の向上が望める。ただし他の解読法に対しては弱くなるおそれはある。また、鍵依存初期線形変換部302 、鍵依存最終線形変換部308 、鍵依存線形変換部347, 353のいずれか、もしくはすべてを鍵に依存しない線形変換部に変更することも可能である。この場合、差分解読法及び線形解読法以外の解読法に対しても安全性が低下しない一方で、インプリメントを最適化することにより、暗号化処理速度の向上が望める。なお、線形変換部としては、ビット位置を予め決めた関係で入れかえる転置、予め決めたビット数だけ回転シフトするなどを行う。鍵依存線形変換部は、鍵データに応じたビット数だけ回転シフトする、あるいは、鍵データとの排他的論理和演算を行うものなどである。

実施例２

図６は、図３の第１実施例の非線形関数部304 （図４）における２段目の４つの非線形変換部348～351のうち、中央の２つを省略した実施例を示す。この実施例では更に、図３における鍵依存初期線形変換部302 と鍵依存最終線形変換部308 も省略している。

平文に相当する入力データＰを入力部301 から暗号装置内に入力する。入力データＰは初期分割部303 で２つのブロックデータL_0, R_0に分割される。ブロックデータR_0は、鍵記憶部322 に保持されている鍵データk_{00}, k_{20}と共に第０段ラウンド処理部３８０の非線形関数部304 に入力され、非線形関数部304 で変換処理を受けて、データＹ０に変換される。データＹ０とデータＬ０は線形演算部30

5 で演算され、データL_0^* に変換される。データL_0^* とデータR_0 は交換部306でデータ位置のスワップが行われ、$L_1=R_0$, $R_1=L_0^*$ とされる。以下、第 i 段ラウンド処理部３８$_i$ (i=1, …, n-1) において２つのデータL_i, R_iについて上記と同様の処理を繰り返し行う。即ち、２つのデータL_i, R_iについて、データR_i は、鍵記憶部322 に保持されている鍵データk_{0i}, k_{2i}と共に非線形関数部304 に入力され、非線形関数部304 で変換処理を受けて、データY_i に変換される。データY_i とデータL_i は線形演算部305 で演算され、データL_i^* に変換される。データL_i^* とデータR_i は交換部306 でデータ位置の交換が行われ、$L_{i+1}=R_i$, $R_{i+1}=L_i^*$ のように変換される。

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、ｎラウンドの繰り返し処理の結果、データL_n, R_nが得られる。このデータL_n, R_nを最終結合部307 で結合した後、出力部309 から暗号文として出力データＣを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。

図７Ａは、図６の実施例における第 i 段ラウンド処理部３８$_i$ の非線形関数部304 の機能構成を示す。前段からの入力データR_i は、鍵記憶部322 に保持されている鍵データk_{0i}, k_{2i}と共に非線形関数部304 への入力データとなる。データR_i は、鍵依存線形変換341 において、データk_{0i}によりデータR_i^* に線形変換される。次に、データR_i^* は分割部342 において４つのデータin_0 , in_1 , in_2 , in_3 に分割される。４つのデータin_0 , in_1 , in_2 , in_3 は、それぞれ非線形変換部343, 344, 345, 346において、データmid_{00}, mid_{01}, mid_{02}, mid_{03}に非線形変換された後、線形変換部354 に入力される。線形変換部354 では、例えば図７Ｂに示すように４つの処理系列３０$_0$～３０$_3$間でデータ相互に関連づけるように変換される。これは図５中の鍵データとの論理演算を省略した場合と同じ例であり、下記の式で表わせる。

$$mid_{10} = mid_{00} \oplus mid_{02} \oplus mid_{03}$$

$$mid_{11} = mid_{02} \oplus mid_{03}$$

$$mid_{12} = mid_{00} \oplus mid_{01} \oplus mid_{02} \oplus mid_{03}$$

$$mid_{13} = mid_{00} \oplus mid_{01} \oplus mid_{02} \quad (12)$$

この線形変換で、均質化されたデータmid_{10}，mid_{11}，mid_{12}，mid_{13}が生成され、そのうちのデータmid_{10}，mid_{13}は、それぞれ非線形変換部348，351において、データout_0，out_3に非線形変換された後、結合部352 において、４つのデータout_0，mid_{11}，mid_{12}，out_3 が１つのデータY_i^* に結合される。最後に、データY_i^* は、データk_{2i}による鍵依存線形変換部353 において、データY_i に線形変換され、非線形関数部304 からの出力データY_i が生成される。

非線形変換部343～346は４つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換部348，351についても同様のことがいえる。この実施例では、各非線形関数部304 内の２段目の非線形変形部が外側の２つ（348，351）だけに減らされているため、それだけ暗号化又は復号化処理量を削減することができる。

なお、鍵データk_i は、鍵入力部320 から暗号装置内に入力された鍵情報Ｋｅｙから鍵データ生成部321 によって変換され、鍵記憶部322 に保持されたデータである。

上記のように構成された暗号装置の場合、例えば、非線形変換部343～346，348，351が差分解読法及び線形解読法に対して確率$p_b=2^{-6}$で近似表現できるように設計されているならば、実施例１と同様に各ラウンドは確率$p_i \leqq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数ｎをn=3mとして、確率$p \leqq 2^{-24m}$ で近似表現できることになる。ここで、例えば m=4（ラウンド数１２段）とすると、$P \leqq 2^{-96}$となり、差分解読法及び線形解読法に対して十分安全な暗号装置となる。

また、鍵依存線形変換部353 があるため、差分解読法と線形解読法以外の解読法に対しても安全性にマージンがある構造であり、かつ実施例１よりも構造が簡素化されているため、処理量が軽減されている。つまり、安全性と低処理量のバランスを重視した暗号装置である。

実施例３

図８は、図６の第２実施例の非線形関数部304 において鍵依存線形変換部353を省略した実施例を示す。平文に相当する入力データＰを入力部301 から暗号装

置内に入力する。入力データＰは初期分割部303 で２つのブロックデータL_0, R_0に分割される。ブロックデータR_0は、鍵記憶部322 に保持されている鍵データk_0と共に第０段ラウンド処理部３８$_0$の非線形関数部304 に入力され、非線形関数部304 で変換処理を受けて、データY_0に変換される。データY_0とデータL_0は線形演算部305 で演算され、データL_0^*に変換される。データL_0^*とデータR_0は交換部306 でデータ位置の交換が行われ、$L_1=R_0$, $R_1=L_0^*$のように変換される。以下、第ｉ段ラウンド処理部３８$_i$では、２つの入力ブロックデータL_i, R_iについて上記と同様の処理を繰り返し行う。即ち、２つのデータL_i, R_iについて、データR_iは、鍵記憶部322 に保持されている鍵データk_iと共に非線形関数部304 に入力され、非線形関数部304 で変換処理を受けて、データY_iに変換される。データY_iとデータL_iは線形演算部305 で演算され、データL_i^*に変換される。データL_i^*とデータR_iは交換部306 でデータ位置の交換が行われ、$L_{i+1}=R_i$, $R_{i+1}=L_i^*$とされ、ブロックデータL_{i+1}, R_{i+1}が出力される。

暗号方式としての安全性を確保するための適切な繰り返し回数をｎとすると、繰り返し処理の結果、データL_n, R_nが得られる。このデータL_n, R_nを最終結合部307 で結合した後、出力部309 から暗号文として出力データＣを出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文Ｃから平文Ｐが得られる。

図９は、図８の実施例における非線形関数部304 の機能構成を示す。非線形関数部304 への入力データR_iは、鍵記憶部322 に保持されている鍵データk_iと共に鍵依存線形変換341 への入力となる。データR_iは、鍵依存線形変換341 において、鍵データk_iによりデータR_i^*に線形変換される。次に、データR_i^*は分割部342 において４つのデータin_0, in_1, in_2, in_3に分割される。４つのデータin_0, in_1, in_2, in_3は、それぞれ非線形変換部343, 344, 345, 346において、データ$mido_0$, $mido_1$, $mido_2$, $mido_3$に非線形変換された後、線形変換部354 に入力される。線形変換部354 では、例えば実施例２の図７Ｂと同じように、

$$mid_{10} = mido_0 \oplus mido_2 \oplus mido_3$$

$$mid_{11} = mido_2 \oplus mido_3$$

$$mid_{12} = mido_0 \oplus mido_1 \oplus mido_2 \oplus mido_3$$

$$mid_{13} = mid_{00} \oplus mid_{01} \oplus mid_{02} \quad (13)$$

に線形変換し、データmid_{10}，mid_{11}，mid_{12}，mid_{13}を生成する。ついで、データmid_{10}，mid_{13}は、それぞれ非線形変換部348，351において、データout_0，out_3に非線形変換された後、結合部352 において、４つのデータout_0，mid_{11}，mid_{12}，out_3が１つのデータに結合され、非線形関数部304 からの出力データY_i が生成される。

非線形変換部343～346は４つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換部348，351についても同様のことがいえる。

なお、鍵データk_i は、鍵入力部320 から暗号装置内に入力された鍵情報Keyから鍵データ生成部321 によって変換され、鍵記憶部322 に保持されたデータである。

上記のように構成された暗号装置の場合、例えば、非線形変換部343～346，348，351が差分解読法及び線形解読法に対して確率$p_b = 2^{-6}$で近似表現できるように設計されているならば、各ラウンドは確率$p_i \leqq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数ｎをn=3mとして、確率$P \leqq 2^{-24m}$ で近似表現できることになる。ここで、例えば m=4（ラウンド数１２段）とすると、$P \leqq 2^{-96}$となり、差分解読法及び線形解読法に対して十分安全な暗号装置となる。

また、差分解読法及び線形解読法に対して十分な安全性を確保するために最低限必要な部しか実行しない構造であるため、処理量が軽減されており、かつ暗号化又は復号化速度もそれだけ改善されている。

上述において、非線形関数部304 中の各分割部342 は４分割に限らず、任意の複数に分割してもよい。なお、４分割の場合においては、第２の非線形変換部は図７Ａ及び図９に示したように２つのみとすることができる。

上述した第２及び第３実施例で示した非線形関数部304 （ラウンド関数）における非線形変換部が６個（343～346，348，351）の場合について、１ラウンド段当たりの安全強度と、安全性条件を満たすラウンド段数と、それに必要な処理量（ステップ数）を図１及び２に示したＤＥＳ暗号装置の場合と比較して次の表に示す。ただし、この発明の実施例ではＤＥＳのS-box に対応する非線形変換部34

3 ～346 への入力データの全ビット数を３２とし、従って、各非線形変換部への入力データは８ビットとしたため、これとサイズを合わせるため、ＤＥＳの各S-box のサイズを８ビットとし、従ってS-box の数を４個として比較した。

比較表

	１段当たりのS-box 数	１段当たりの安全性強度	必要な段数	ステップ数
ＤＥＳ	4	2^{-6}	１７	６８
この発明	6	2^{-12}	9	５４

この表からわかるように、１段当たりのS-box の個数（非線形変換部の数）が、この発明の方がＤＥＳより多いにもかかわらず、この発明の１ラウンド段当たりの安全性強度はＤＥＳの２倍となっている。そのため安全性条件を満たすためのラウンド段数はＤＥＳの場合より少なくなっており、またその安全性に必要な処理量（ステップ数）も少なくなっている。

発明の効果

以上、詳細に説明したように、この発明によれば、非線形関数部で入力データを複数に分割し、かつそれぞれ非線形変換を行い、その後、相互に線形交換を行い、更に少くとも一部を非線形変換することによりデータの通信または保持においてデータを秘匿するための暗号装置について、安全性が高い暗号装置を提供することができる。

請求の範囲

1．鍵データを使って非線形変換を行う複数段のラウンド処理により入力データを順次処理して暗号化する暗号化装置であり、

入力データを２つのブロックデータに分割する初期分割部と、

鍵データを保持する鍵記憶部と、

上記２つのブロックデータが入力され、上記鍵データを使い順次処理を行う縦続接続された複数段のラウンド処理部と、

縦続接続された上記複数のラウンド処理部の最終段から出力される２つのブロックデータを１つのデータに結合し、その結合データを出力する最終結合部と、

を含み、

各段の上記ラウンド処理部は：

前段から入力された２つのブロックデータの一方に対し、上記鍵記憶部に保持された鍵データに依存したデータ変換処理を行う非線形関数部と、

上記非線形関数部の出力データと、入力された上記２つのブロックデータの他方とを線形演算する線形演算部と、

上記線形演算部の出力データと上記非線形関数部への入力ブロックデータとを交換し、交換された２つのデータを次段の上記ラウンド処理部に２つの入力ブロックデータとして与える交換部と、

を含み、

上記非線形関数部は：

入力されたデータに上記鍵記憶部に保持された鍵データに基づいて線形変換を行い、変換データを生成する鍵依存線形変換部と、

上記鍵依存線形変換部からの変換データを複数個のビット列に分割する分割部と、

これらのビット列をそれぞれ非線形変換して変換データを出力する複数の第１非線形変換部と、

上記複数の第１非線形変換部からの変換データ間で線形変換を行い、均質化された複数のデータを複数の系列にそれぞれ出力する第１の線形変換部と、

上記複数の系列の少なくとも１つに設けられ、対応する上記第１線形変換部からの上記均質化されたデータに非線形変換を行い、変換データをその系列のデータとして出力する第２の非線形変換部と、

上記複数の系列からのデータを結合して上記非線形関数部の出力データとする結合部と、

を含む。

２．請求項１に記載の暗号装置において、上記第１の線形変換部は、上記均質化された複数のデータを上記鍵記憶部に保持された鍵データに基づいて線形変換し、上記複数の系列のデータとして出力する鍵依存線形演算部を含む。

３．請求項１又は２に記載の暗号装置において、上記結合部の出力データを線形変換して上記非線形関数部の出力データとする第２の線形変換部が設けられている。

４．請求項３に記載の暗号装置において、上記第２の線形変換部は、上記鍵記憶部に保持された鍵データに基づいて線形変換を行う線形変換部である。

５．請求項４に記載の暗号装置において、上記第１線形変換部は、各上記系列に少なくとも１つ設けられ、その系列のデータと他の系列のデータとの排他的論理和演算により上記均質化されたデータをその系列に出力する排他的論理和を含む。

６．請求項１乃至５のいずれかに記載の暗号装置において、上記入力データに線形変換を行って上記初期分割部へ供給する初期線形変換部が設けられている。

７．請求項６に記載の暗号装置において、上記初期線形変換部は上記鍵記憶部に保持された鍵データに基づいて線形変換を行う変換部である。

８．請求項１乃至７のいずれかに記載の暗号装置において、上記最終結合部の出力データに線形変換を行って暗号装置の出力とする最終線形変換部が設けられている。

９．請求項８に記載の暗号装置において、上記最終線形変換部は上記鍵記憶部に保持された鍵データに基づいて線形変換を行う変換部である。

１０．請求項１乃至９のいずれかに記載の暗号装置において、上記複数の系列は第１、第２、第３及び第４系列の順に次配列された４系列である。

１１．請求項１０に記載の暗号装置において、上記第２非線形変換部は上記４つ

の系列のそれぞれに設けられている。

１２．請求項１０に記載の暗号装置において、上記第２非線形変換部は上記第１及び第４系列にそれぞれ設けられている。

１３．請求項１２に記載の暗号装置において、上記第１線形変換部は：

上記第２系列に設けられ、上記第１系列のデータと第２系列のデータの排他的論理和を演算する第１排他的論理和と、

上記第３系列に設けられ、上記第４系列のデータと第３系列のデータの排他的論理和を演算する第２排他的論理和と、

上記第３系列に設けられ、上記第２排他的論理和の出力と上記第１排他的論理和の出力との排他的論理和を演算する第３排他的論理和と、

上記第２系列に設けられ、上記第１排他的論理和の出力と上記第３排他的論理和の出力との排他的論理和を演算する第４排他的論理和と、

上記第１系列に設けられ、上記第１系列のデータと上記第４排他的論理和の出力との排他的論理和を演算する第５排他的論理和と、

上記第４系列に設けられ、上記第４系列のデータと上記第３排他的論理和の出力との排他的論理和を演算する第６排他的論理和と、

を含む。

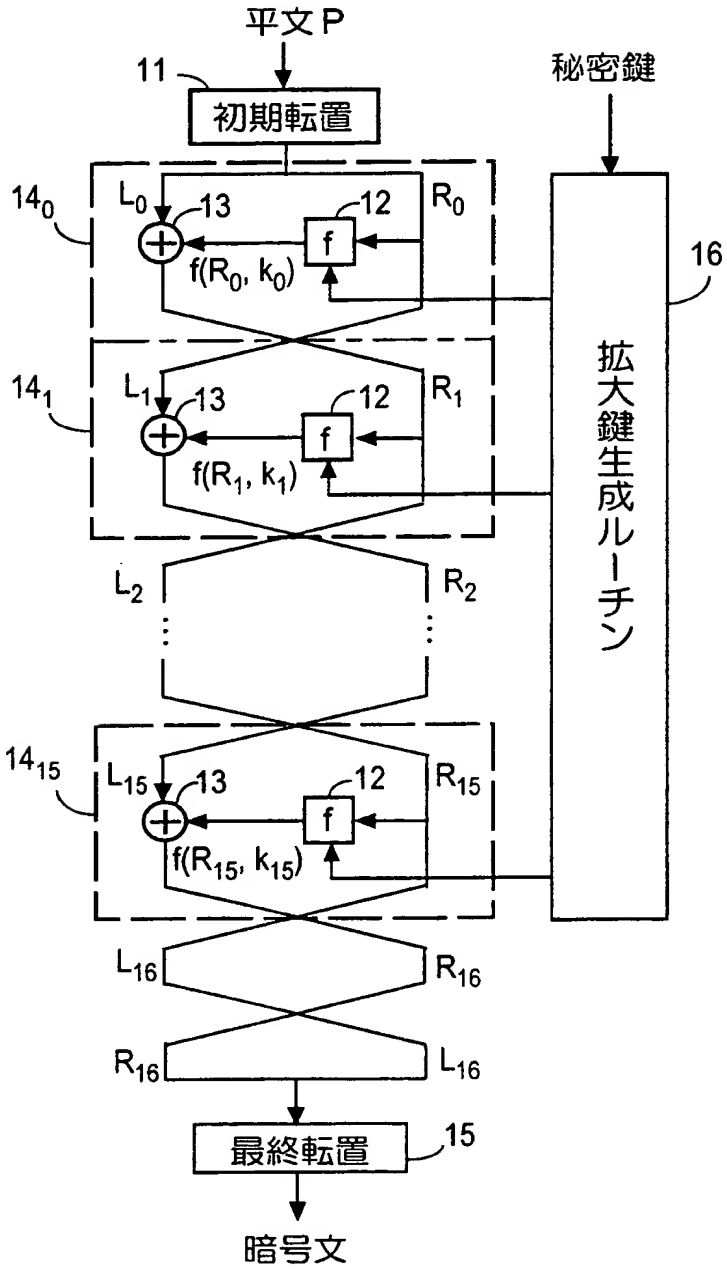

平文P
11
初期転置
秘密鍵
14_0
L_0
13
12
R_0
f
$f(R_0, k_0)$
16
14_1
L_1
13
12
R_1
f
$f(R_1, k_1)$
拡大鍵生成ルーチン
L_2
R_2
14_{15}
L_{15}
13
12
R_{15}
f
$f(R_{15}, k_{15})$
L_{16}
R_{16}
R_{16}
L_{16}
最終転置
15
暗号文

図1

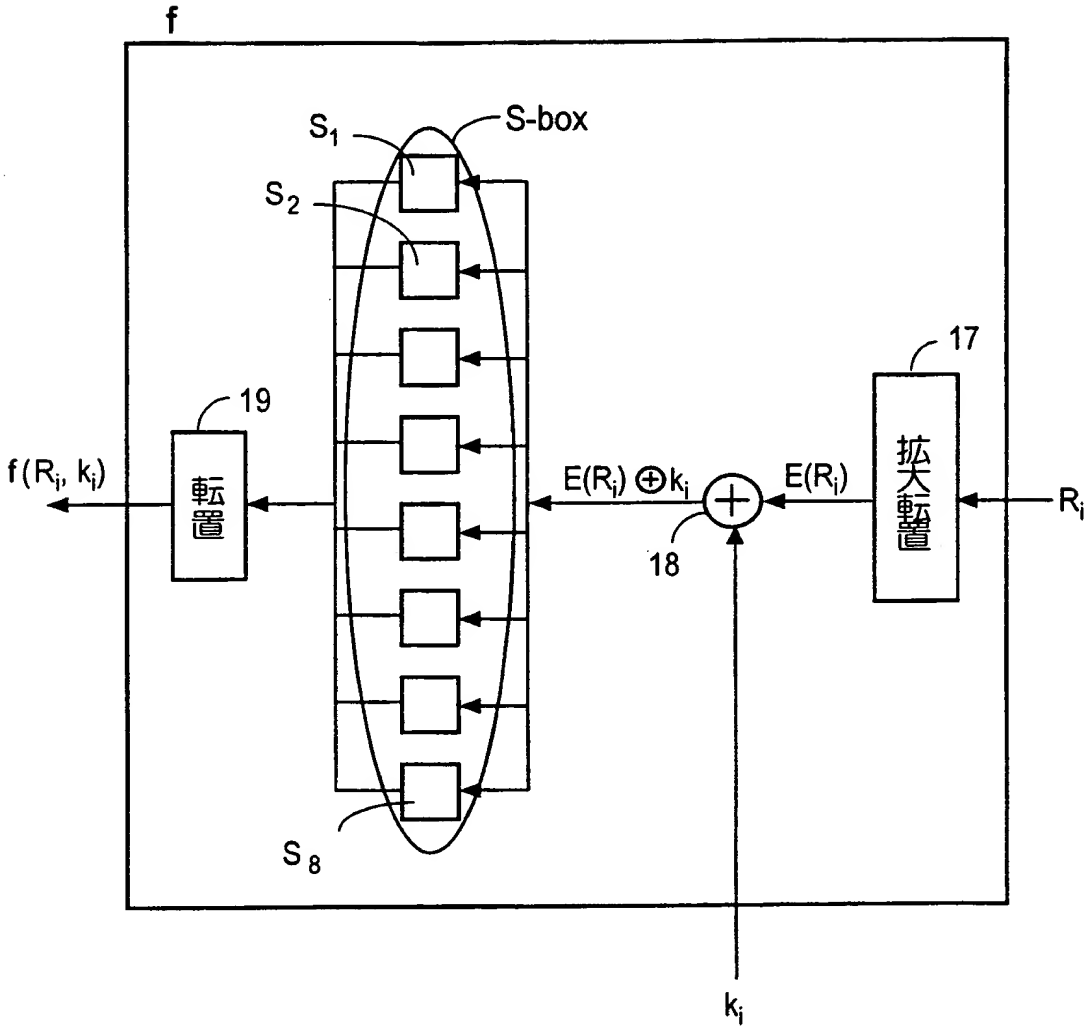


図2

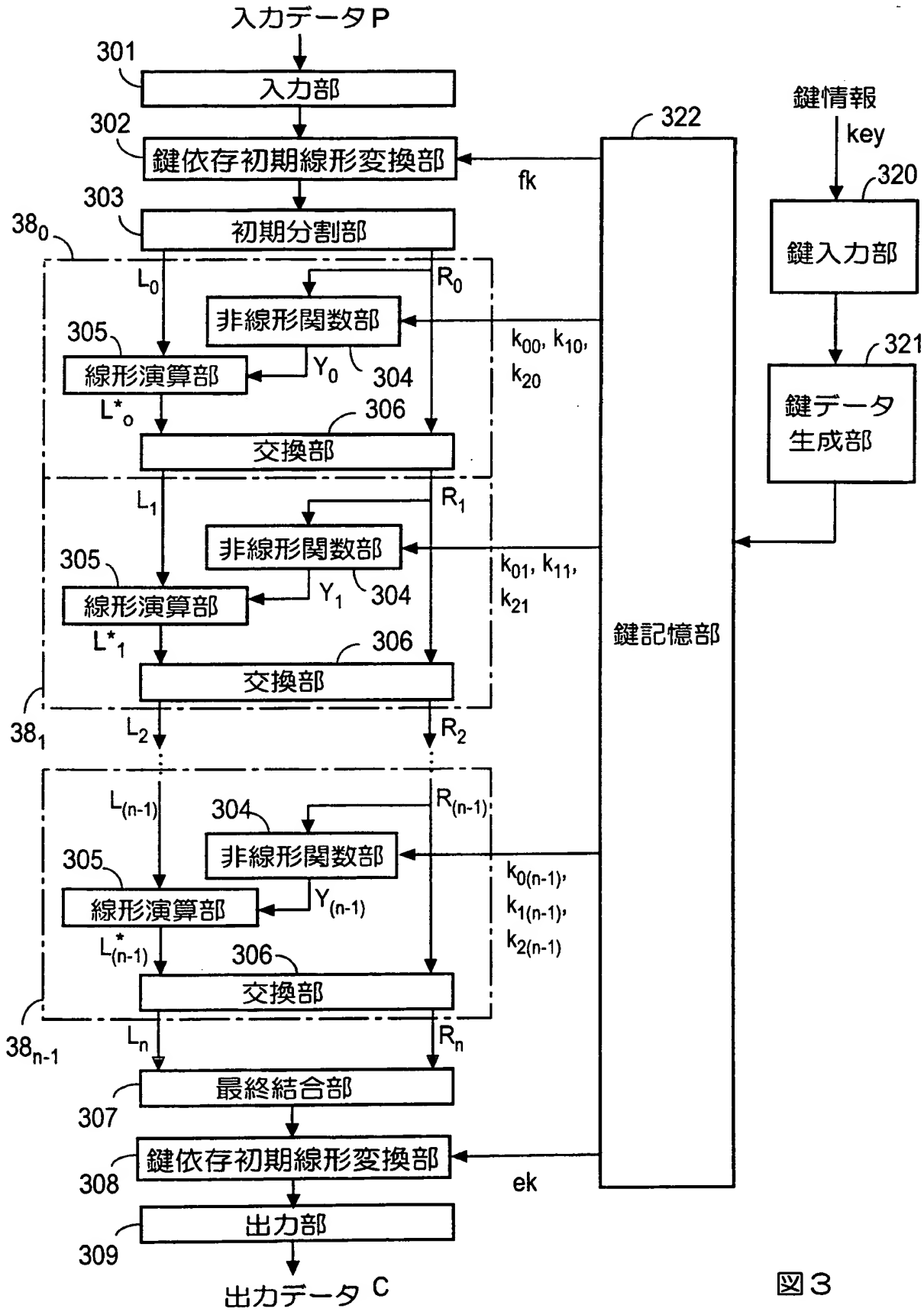

入力データP
301
入力部
302
鍵依存初期線形変換部
303
初期分割部
38_0
L_0
R_0
非線形関数部
305
線形演算部
Y_0
304
L^*_0
306
交換部
L_1
R_1
非線形関数部
305
線形演算部
Y_1
304
L^*_1
306
交換部
38_1
L_2
R_2
$L_{(n-1)}$
304
$R_{(n-1)}$
非線形関数部
305
線形演算部
$Y_{(n-1)}$
$L^*_{(n-1)}$
306
交換部
38_{n-1}
L_n
R_n
最終結合部
307
鍵依存初期線形変換部
308
出力部
309
出力データC
fk
k_{00}, k_{10}, k_{20}
k_{01}, k_{11}, k_{21}
$k_{0(n-1)}$, $k_{1(n-1)}$, $k_{2(n-1)}$
ek
322
鍵記憶部
鍵情報
key
320
鍵入力部
321
鍵データ生成部

図3

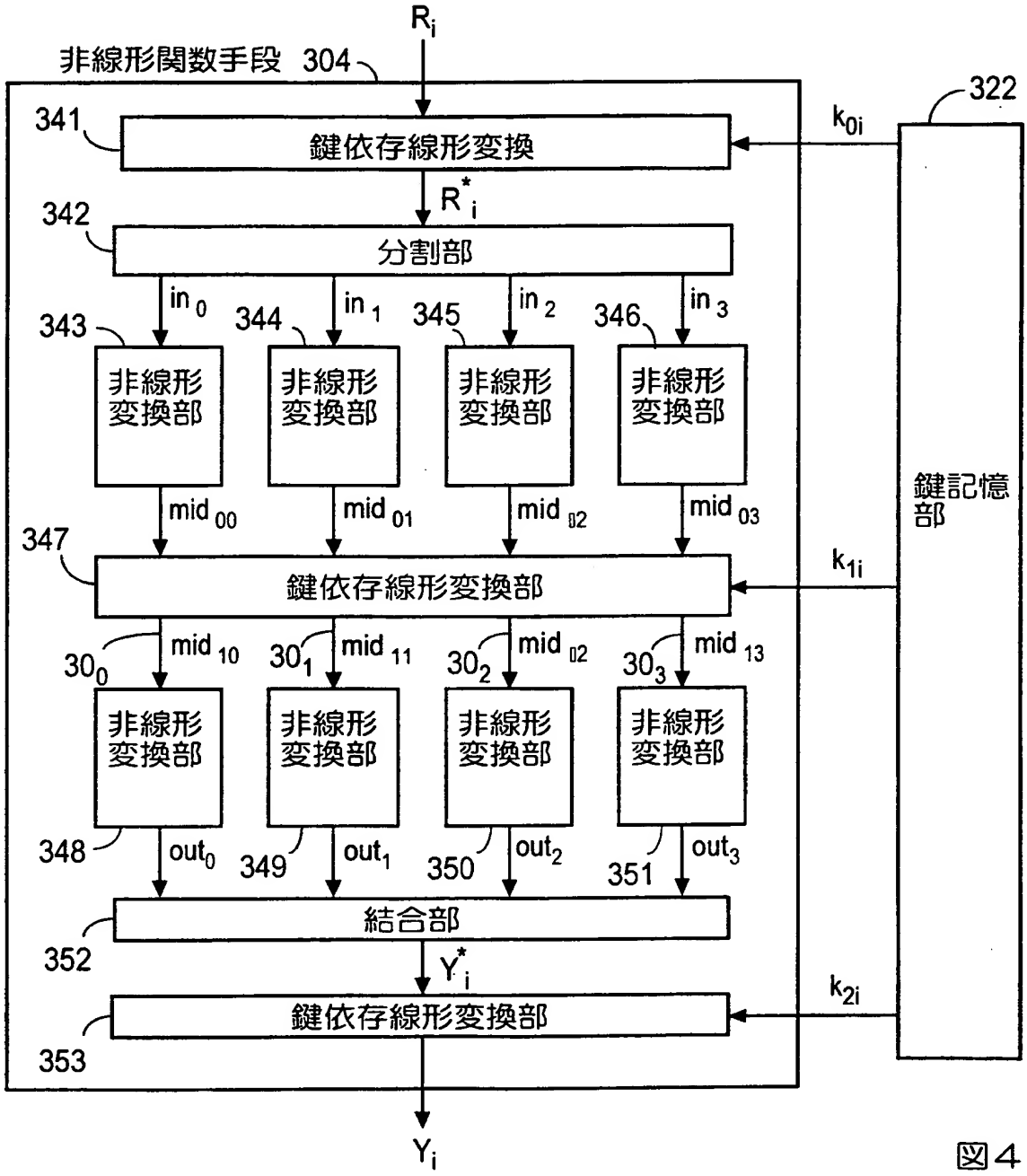

R_i
非線形関数手段 304
322
341
鍵依存線形変換
k_0i
R*_i
342
分割部
in_0
in_1
in_2
in_3
343
344
345
346
非線形変換部
非線形変換部
非線形変換部
非線形変換部
鍵記憶部
mid_00
mid_01
mid_02
mid_03
347
鍵依存線形変換部
k_1i
mid_10
mid_11
mid_12
mid_13
30_0
30_1
30_2
30_3
非線形変換部
非線形変換部
非線形変換部
非線形変換部
348
349
350
351
out_0
out_1
out_2
out_3
結合部
352
Y*_i
k_2i
鍵依存線形変換部
353
Y_i

図4

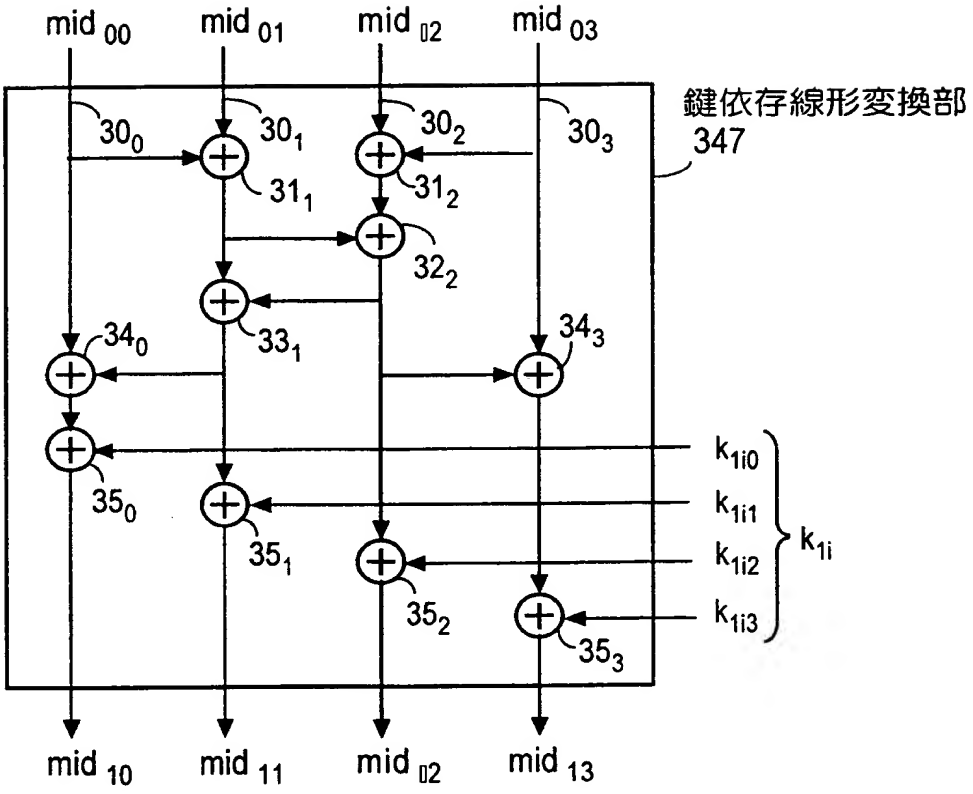

mid 00
mid 01
mid 02
mid 03
鍵依存線形変換部
347
30 0
30 1
30 2
30 3
31 1
31 2
32 2
33 1
34 0
34 3
35 0
35 1
35 2
35 3
k 1i0
k 1i1
k 1i2
k 1i3
k 1i
mid 10
mid 11
mid 02
mid 13

図5

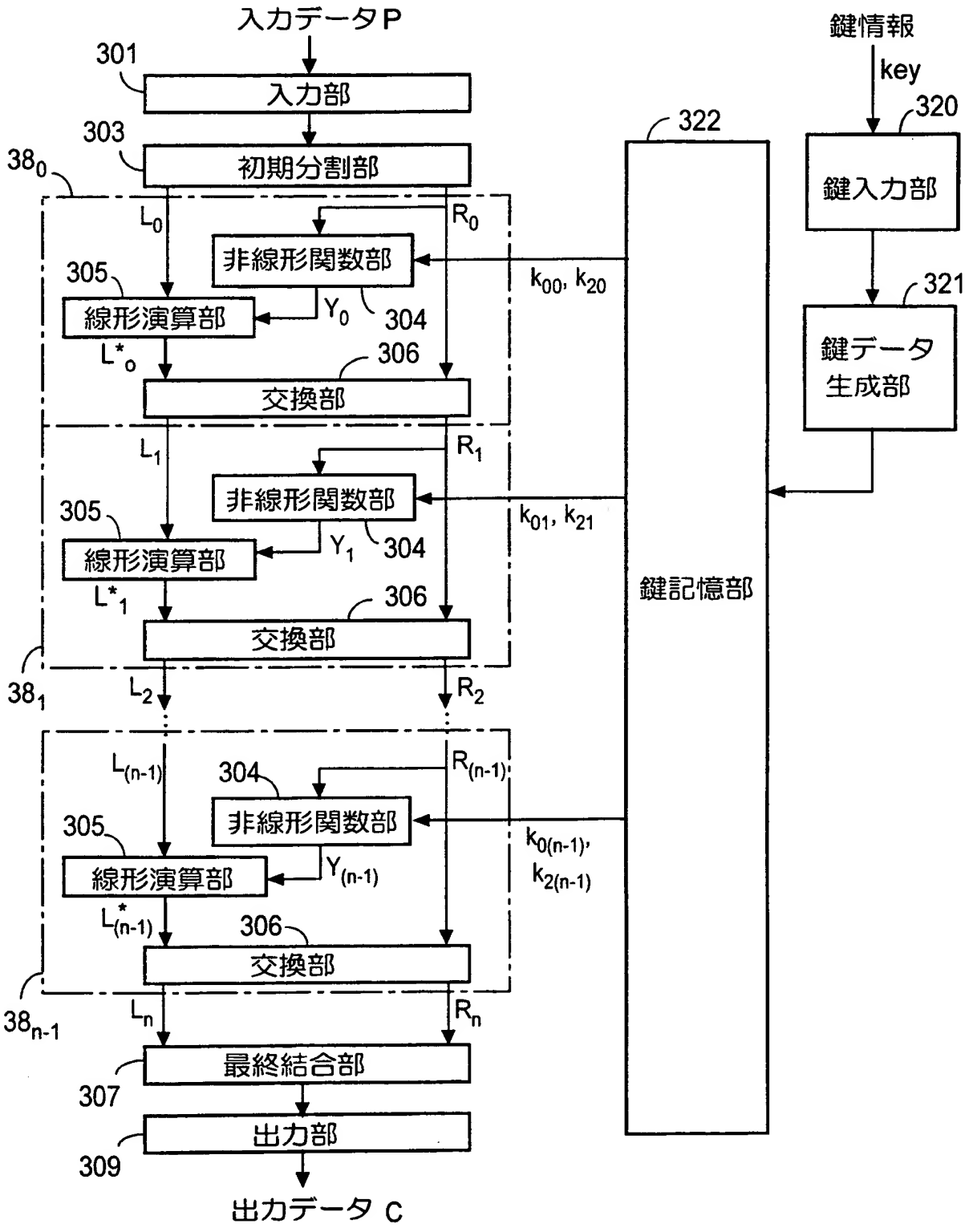

入力データP
301
入力部
303
初期分割部
38_0
L_0
R_0
非線形関数部
305
線形演算部
Y_0
304
L^*_0
306
交換部
L_1
R_1
非線形関数部
305
線形演算部
Y_1
304
L^*_1
306
交換部
38_1
L_2
R_2
$L_{(n-1)}$
$R_{(n-1)}$
304
非線形関数部
305
線形演算部
$Y_{(n-1)}$
$L^*_{(n-1)}$
306
交換部
38_{n-1}
L_n
R_n
最終結合部
307
出力部
309
出力データ C
k_{00}, k_{20}
k_{01}, k_{21}
$k_{0(n-1)}$,
$k_{2(n-1)}$
322
鍵記憶部
鍵情報
key
320
鍵入力部
321
鍵データ
生成部

図6

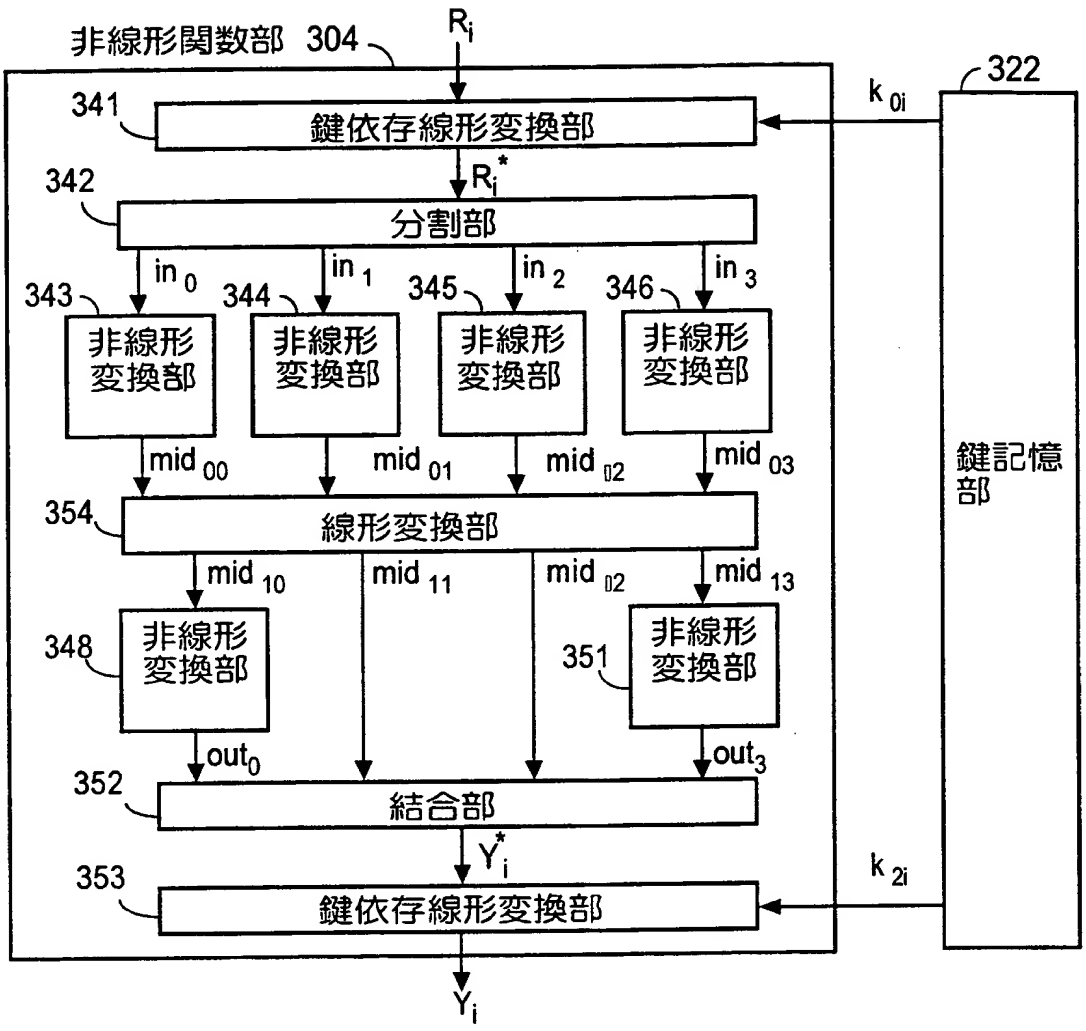

非線形関数部 304
R_i
322
k_{0i}
341
鍵依存線形変換部
R_i^*
342
分割部
in_0
in_1
in_2
in_3
343
344
345
346
非線形変換部
非線形変換部
非線形変換部
非線形変換部
mid_{00}
mid_{01}
mid_{02}
mid_{03}
鍵記憶部
354
線形変換部
mid_{10}
mid_{11}
mid_{02}
mid_{13}
348
351
非線形変換部
非線形変換部
out_0
out_3
352
結合部
Y_i^*
k_{2i}
353
鍵依存線形変換部
Y_i

図7A

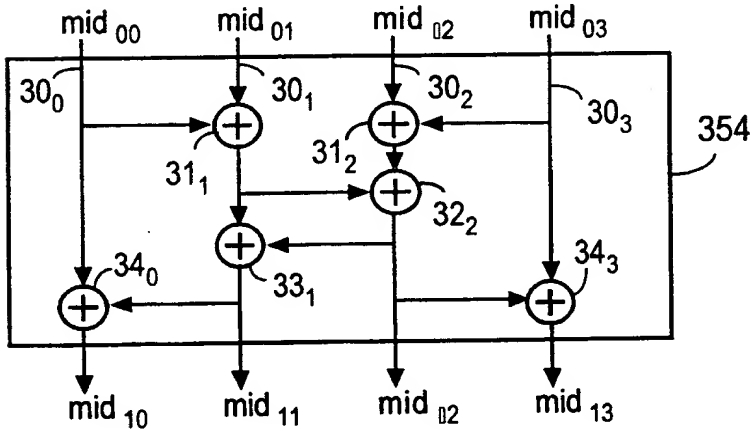

mid_{00}
mid_{01}
mid_{02}
mid_{03}
30_0
30_1
30_2
30_3
354
31_1
31_2
32_2
33_1
34_0
34_3
mid_{10}
mid_{11}
mid_{02}
mid_{13}

図7B

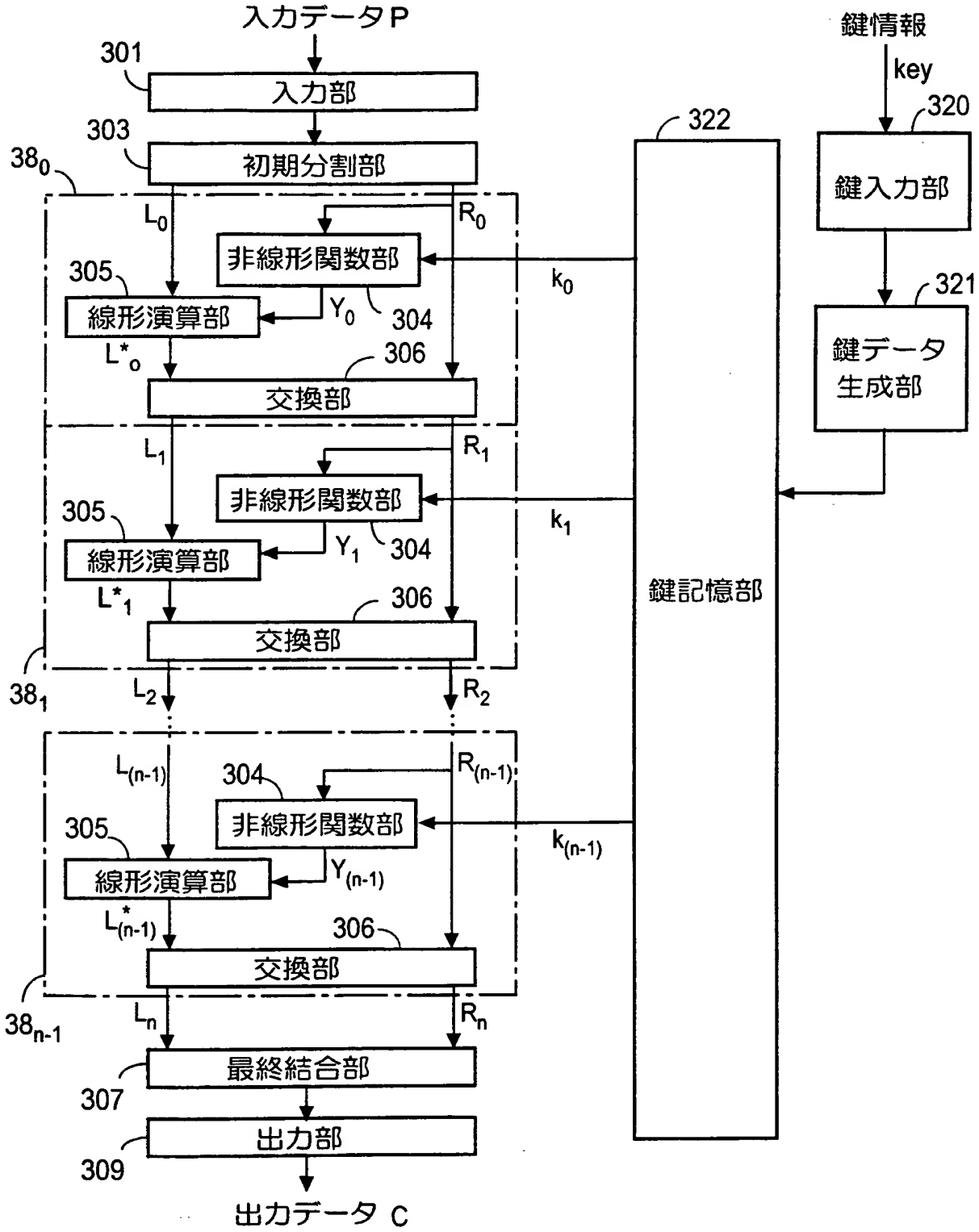

入力データP
301
入力部
303
初期分割部
38_0
L_0
R_0
非線形関数部
305
線形演算部
Y_0
304
L^*_0
306
交換部
L_1
R_1
非線形関数部
305
線形演算部
Y_1
304
L^*_1
306
交換部
38_1
L_2
R_2
$L_{(n-1)}$
$R_{(n-1)}$
304
非線形関数部
305
線形演算部
$Y_{(n-1)}$
$L^*_{(n-1)}$
306
交換部
38_{n-1}
L_n
R_n
最終結合部
307
出力部
309
出力データ C
k_0
k_1
$k_{(n-1)}$
322
鍵記憶部
鍵情報
key
320
鍵入力部
321
鍵データ生成部

図8

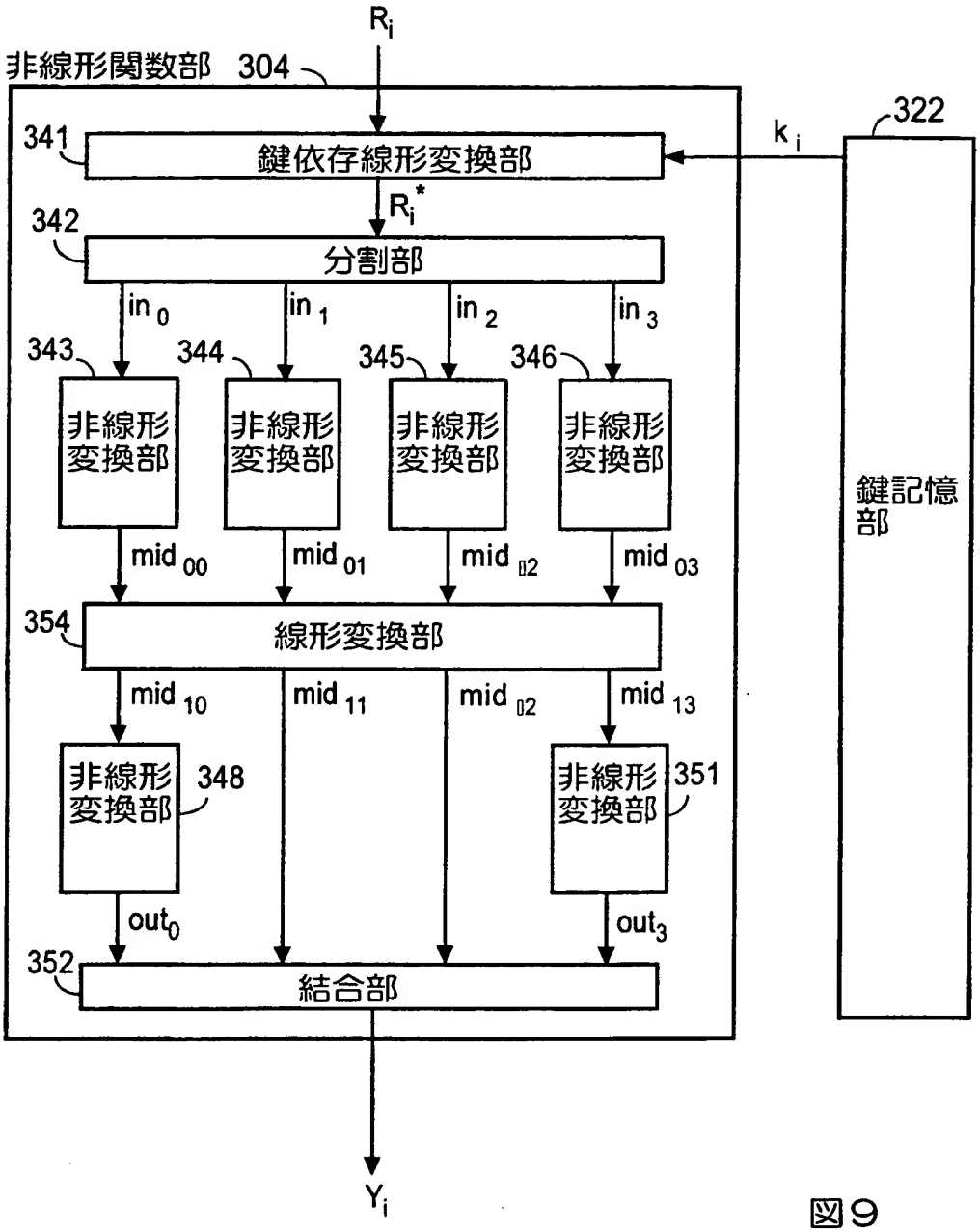

R_i
非線形関数部 304
341
鍵依存線形変換部
k_i
322
R_i^*
342
分割部
in_0
in_1
in_2
in_3
343
344
345
346
非線形変換部
非線形変換部
非線形変換部
非線形変換部
鍵記憶部
mid_{00}
mid_{01}
mid_{02}
mid_{03}
354
線形変換部
mid_{10}
mid_{11}
mid_{02}
mid_{13}
非線形変換部
348
非線形変換部
351
out_0
out_3
352
結合部
Y_i

図9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/02915

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G09C1/00, H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G09C1/00, H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1998 Jitsuyo Shinan Toroku Koho 1996-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, 98/09705, A1 (Mitsubishi Electric Corp.), 13 March, 1997 (13. 03. 97), Full text ; Figs. 1 to 29 & AU, 6629396, A1 & NO, 972052, A & EP, 790595, A1	1-13
A	Mitsuru Matsui, "Provable Safety of Differential Decoding and Linear Decoding of Block Cipher (in Japanese)", Preprint of the 18th Symposium on Information Theories and their Applications, The Institute of Information Theories and their Applications, Vol. 1 of 2 October 1995 (10. 95) p.175-178	1-13
A	Mitsuru Matsui, et al., "Practical Block Cipher Having Provable Safety of Differential Decoding and Linear Decoding (in Japanese)", Symposium on Cipher and Information Security, SCIS96, Information Security Research Special Committee of IEICE, January 1996 (01. 96) SCIS96-4C	1-13

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September, 1998 (17. 09. 98)	29 September, 1998 (29. 09. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/02915

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 9-54547, A (NEC Corp.), 25 February, 1997 (25. 02. 97), Full text ; Figs. 1 to 11 (Family: none)	1-13
P, A	Masato Kanda, et al., "Structure of Round Function Using a Little S-box (Part 1) (in Japanese)", Technical Research Report of IEICE (ISEC97 14-22), Vol. 97, No. 181, 18 July, 1997 (18. 07. 97) p.41-52	1-13

国際調査報告

国際出願番号　PCT／JP98／02915

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶　G09C1／00, H04L9／06

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶　G09C1／00, H04L9／06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－1998年
日本国登録実用新案公報	1994－1998年
日本国実用新案登録公報	1996－1998年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	WO, 98/09705, A1（三菱電機株式会社） 13.3月.1997(13.03.97) 全文, 第1-29図 & AU, 6629396, A1 & NO, 972052, A & EP, 790595, A1	1-13
A	松井充, ﾌﾞﾛｯｸ暗号の差分解読法と線形解読法に対する証明可能安全性について, 第18回情報理論とその応用ｼﾝﾎﾟｼﾞｳﾑ予稿集, 情報理論とその応用学会, Vol.1 of 2 10月.1995(10.95) p.175-178	1-13

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」先行文献ではあるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 17. 09. 98	国際調査報告の発送日　29.09.98
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木　重徳　印　5J　4229 電話番号　03－3581－1101　内線　3538

様式PCT／ISA／210（第2ページ）（1992年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０２９１５

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	松井充 他，差分解読法と線形解読法に対する証明可能安全性をもつ実用ﾌﾞﾛｯｸ暗号， 暗号と情報ｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑSCIS96講演論文集， 電子情報通信学会情報ｾｷｭﾘﾃｨ研究専門委員会， 1月．1996(01．96) SCIS96-4C	1-13
A	JP，9-54547，A（日本電気株式会社） 25．2月．1997（25．02．97） 全文，第1-11図（ﾌｧﾐﾘｰなし）	1-13
P，A	神田雅透 他，少数のS-boxを用いたﾗｳﾝﾄﾞ関数の構成について(その1)， 電子情報通信学会技術研究報告(ISEC97 14-22)，Vol．97，No．181， 18．7月．1997（18．07．97）p．41-52	1-13

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（１９９２年７月）